

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-72717

(P2004-72717A)

(43) 公開日 平成16年3月4日(2004.3.4)

(51) Int. Cl.⁷

H04L 9/08

H04L 9/32

F I

H04L 9/00

601 F

H04L 9/00

675 D

テーマコード (参考)

5 J 1 0 4

審査請求 未請求 請求項の数 23 O L (全 22 頁)

(21) 出願番号 特願2003-128549 (P2003-128549)
(22) 出願日 平成15年5月7日 (2003.5.7)
(31) 優先権主張番号 特願2002-170798 (P2002-170798)
(32) 優先日 平成14年6月12日 (2002.6.12)
(33) 優先権主張国 日本国 (JP)

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(74) 代理人 100075096
弁理士 作田 康夫
(72) 発明者 鍛 忠司
神奈川県川崎市麻生区王禅寺1099番地
株式会社日立製作所システム開発研究所
内
(72) 発明者 藤城 孝宏
神奈川県川崎市麻生区王禅寺1099番地
株式会社日立製作所システム開発研究所
内

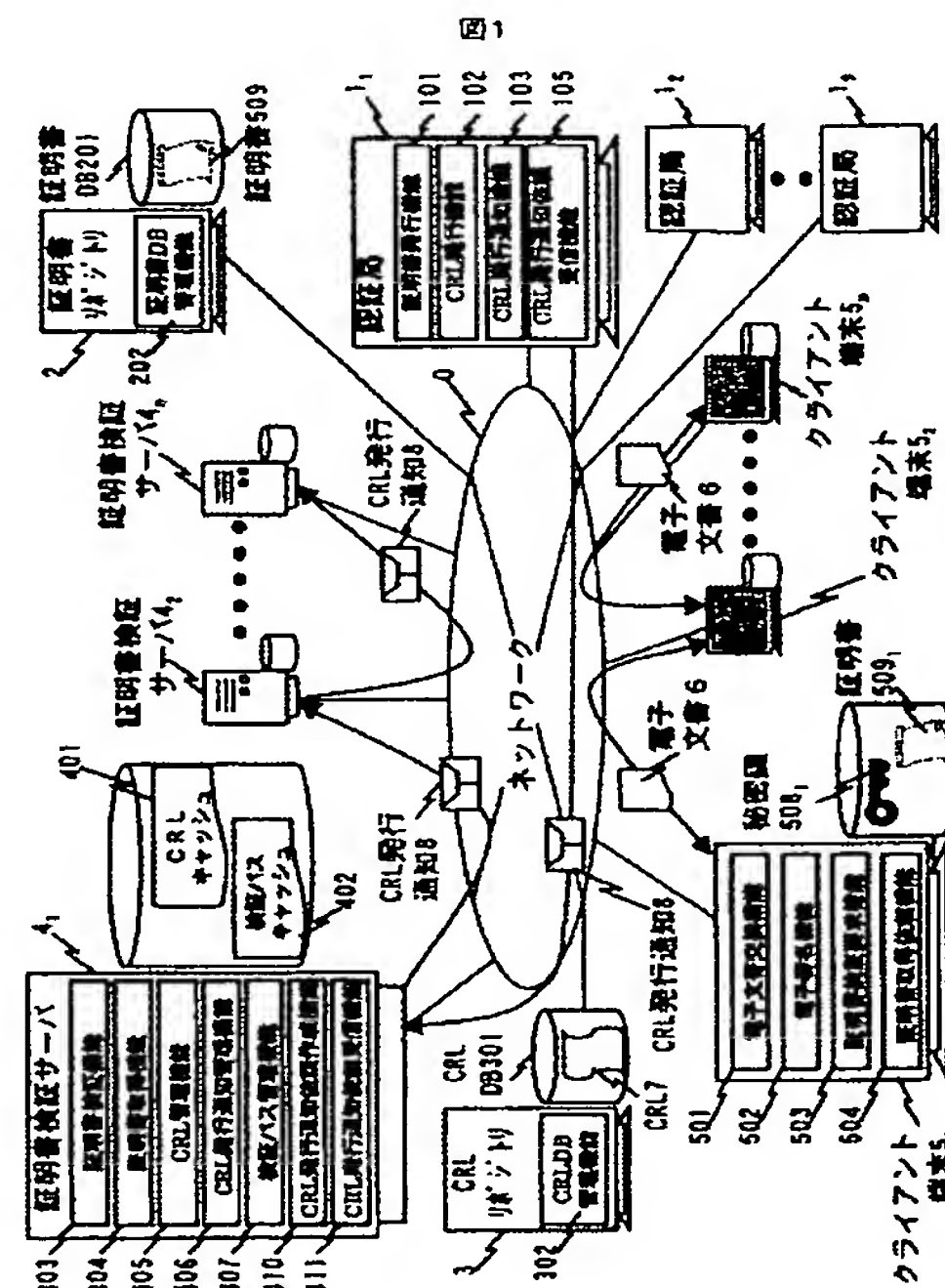
最終頁に続く

(54) 【発明の名称】 C R L発行通知機能付き認証基盤システム

(57) 【要約】

【課題】 証明書の有効性判定処理を高速化するためにC R Lをキャッシュすると、認証局がC R Lを緊急に発行した場合に、キャッシュしている前記C R Lが最新のものではないため、証明書の有効性検証結果の精度が保証できない。

【解決手段】 前記C R Lが発行された場合に、前記認証局から前記証明書検証サーバにC R L発行通知が行われ、かつ、当該C R L発行通知を受信した前記証明書検証サーバは最新の前記C R Lをキャッシュするため、証明書有効性検証結果の精度が保証できる。



【特許請求の範囲】

【請求項1】

証明書を発行する証明書発行手段と、CRLを発行するCRL発行手段とを備えた認証局と、前記認証局が発行した前記CRLを格納するCRL格納手段を備えたCRLリポジトリと、前記証明書の有効性を検証する証明書有効性検証手段と、前記CRLリポジトリから取得した前記CRLをキャッシュするCRLキャッシュ手段とを備えた証明書検証サーバと、を備え、前記認証局は、前記CRLを発行した場合に「CRLが発行された」旨を通知するCRL発行通知を、前記証明書検証サーバに送信するCRL発行通知送信手段を備え、前記証明書検証サーバは、前記認証局から前記CRL発行通知を受信するCRL発行通知受信手段を備えることを特徴とする、認証基盤システム。

【請求項2】

請求項1記載の認証基盤システムであって、前記証明書検証サーバの前記CRLキャッシュ手段は、前記CRL発行通知受信手段によって前記CRL発行通知を受信した場合に、前記認証局が新たに発行した前記CRLを前記CRLリポジトリから取得することを特徴とする認証基盤システム。

【請求項3】

請求項1または2記載の認証基盤システムであって、前記証明書検証サーバは、前記CRLが新たに発行されたことを発見した場合に、予め登録された他の証明書検証サーバに対して、「CRLが発行された」旨を通知する、CRL発行通知送信手段を備えることを特徴とする、認証基盤システム。

【請求項4】

証明書の有効性を検証する証明書有効性検証手段と、当該証明書有効性検証手段が前記証明書の有効性を検証するために構築した検証パスをキャッシュする検証パスキャッシュ手段とを備えた証明書検証サーバと、電子署名を検証する電子署名検証手段と、前記証明書検証サーバに前記証明書の有効性検証を依頼する証明書有効性検証依頼手段を備えたクライアントと、を備え、前記証明書検証サーバは、前記検証パスを構築した場合に、予め登録された他の証明書検証サーバに当該検証パスを送信する検証パス送信手段を備え、前記検証パスキャッシュ手段は、他の証明書検証サーバから前記検証パスを受信した場合に、当該検証パスをキャッシュすることを特徴とする認証基盤システム。

【請求項5】

証明書を発行する証明書発行手段を備えた認証局と、前記認証局が発行した前記証明書を格納する証明書格納手段を備えた証明書リポジトリと、

前記証明書の有効性を検証する証明書有効性検証手段を備えた証明書検証サーバと、電子署名を検証する電子署名検証手段と、前記証明書検証サーバに前記証明書の有効性検証を依頼する証明書有効性検証依頼手段を備えたクライアントと、を備え、前記クライアントは、前記電子署名を検証するために必要な前記証明書の取得を、前記証明書検証サーバに依頼する証明書取得依頼手段を備え、前記証明書検証サーバは、前記クライアントから取得を要求された前記証明書を前記証明書リポジトリから取得し、かつ、前記証明書検証手段によって、当該証明書が有効であると判定された場合に、前記クライアントに当該証明書を送信する証明書取得手段を備えることを特徴とする認証基盤システム。

【請求項6】

証明書を発行する証明書発行手段と、CRLを発行するCRL発行手段とを備え、前記CRLを発行すると同時に、前記証明書検証サーバに「CRLが発行された」旨を通知するCRL発行通知を送信するCRL発行通知送信手段を備えることを特徴とする認証局。

【請求項7】

証明書の有効性を検証する証明書有効性検証手段と、CRLをキャッシュするCRLキャッシュ手段とを備え、CRLが発行されたことを通知するCRL発行通知を受信するCRL発行通知受信手段、を備えることを特徴とする、証明書検証サーバ。

【請求項8】

請求項7記載の証明書検証サーバであって、前記証明書検証サーバの前記CRLキャッシュ手段は、前記CRL発行通知受信手段によって、前記CRL発行通知を受信した場合に、新たに発行した前記CRLを取得することを特徴とする証明書検証サーバ。

【請求項9】

請求項7または8記載の証明書検証サーバであって、前記CRLが新たに発行されたことを発見した場合に、予め登録された他の証明書検証サーバに対して、「CRLが発行された」旨を通知するCRL発行通知送信手段を備えることを特徴とする証明書検証サーバ。

【請求項10】

証明書の有効性を検証する証明書有効性検証手段と、当該証明書有効性検証手段が前記証明書の有効性を検証するために構築した検証パスをキャッシュする検証パスキャッシュ手段とを備え、前記検証パスを構築した場合に、予め登録された他の証明書検証サーバに当該検証パスを送信する検証パス送信手段を備え、前記検証パスキャッシュ手段は、他の証明書検証サーバ

から前記検証パスを受信した場合に、当該検証パスをキャッシュする

ことを特徴とする証明書検証サーバ。

【請求項 1 1】

電子署名を検証する電子署名検証手段と、証明書検証サーバに前記証明書の有効性検証を依頼する証明書有効性検証依頼手段を備え、

前記電子署名を検証するために必要な前記証明書の取得を、前記証明書検証サーバに依頼する証明書取得依頼手段を備える

ことを特徴とするクライアント装置。

【請求項 1 2】

前記証明書の有効性を検証する証明書有効性検証手段を備え、

取得を要求された前記証明書を前記証明書リポジトリから取得し、かつ、前記証明書検証手段によって当該証明書が有効であると判定された場合に、当該証明書を返信する証明書取得手段を備える

ことを特徴とする証明書検証サーバ。

【請求項 1 3】

請求項 1 記載の認証基盤システムであって、

前記証明書検証サーバは、C R L 発行通知依頼メッセージを作成する、C R L 発行通知依頼作成手段を備え

前記認証局は、前記 C R L 発行通知依頼メッセージを受信する、C R L 発行通知依頼受信手段を備え、

前記認証局の前記 C R L 発行通知送信手段は、当該認証局に対して前記 C R L 発行通知依頼メッセージを送信してきた証明書検証サーバに対して、前記 C R L 発行通知を送信する。

【請求項 1 4】

請求項 1 3 記載の認証基盤システムであって、

前記証明書検証サーバは、

他の証明書検証サーバから前記 C R L 発行通知依頼メッセージを受信する、C R L 発行通知依頼受信手段と、

前記 C R L 発行通知を受信した場合に、前記 C R L 発行通知依頼メッセージを送信してきた証明書検証サーバに対して、前記 C R L 発行通知を転送する、C R L 発行通知管理手段を備える。

【請求項 1 5】

請求項 6 記載の認証局であって、

C R L 発行通知依頼メッセージを受信する、C R L 発行通知依頼受信手段を備え、

前記 C R L 発行通知送信手段は、前記 C R L 発行通知を受信した前記 C R L 発行通知依頼メッセージの送信元に送信する。

【請求項 1 6】

請求項 7 記載の証明書検証サーバであって、

C R L 発行通知依頼メッセージを作成する、C R L 発行通知依頼作成手段を備える。

【請求項 1 7】

(3)

特開 2 0 0 4 - 7 2 7 1 7

請求項 1 6 記載の証明書検証サーバであって、

他の証明書検証サーバから前記 C R L 発行通知依頼メッセージを受信する、C R L 発行通知依頼受信手段と、

前記 C R L 発行通知を受信した場合に、前記 C R L 発行通知依頼メッセージを送信してきた証明書検証サーバに対して、前記 C R L 発行通知を転送する、C R L 発行通知管理手段を備える。

【請求項 1 8】

認証局が発行した C R L を格納する C R L 格納手段を備えた C R L リポジトリであって、

前記 C R L 格納手段が、新たな C R L を格納すると、C R L 発行通知を送信する C R L 発行通知送信手段を備える。

【請求項 1 9】

請求項 1 8 記載の C R L リポジトリであって、

C R L 発行通知依頼メッセージを受信する、C R L 発行通知依頼受信手段を備え、

前記 C R L 発行通知送信手段は、前記 C R L 発行通知を受信した前記 C R L 発行通知依頼メッセージの送信元に送信する。

【請求項 2 0】

計算機に、C R L の発行を監視し、新たな C R L が発行された場合に、C R L 発行通知を送信する C R L 発行通知送信手段を実現する、C R L 発行確認ソフトウェアであって、

C R L 発行通知依頼メッセージを受信する、C R L 発行通知依頼受信手段を実現し、

前記 C R L 発行通知送信手段は、前記 C R L 発行通知を受信した前記 C R L 発行通知依頼メッセージの送信元に送信する。

【請求項 2 1】

「C R L が発行された」旨を通知する、C R L 発行通知用データフォーマットであって、

新たに発行された C R L 自身を記載する項目を含む。

【請求項 2 2】

「C R L が発行された」旨を通知する、C R L 発行通知用データフォーマットであって、

当該発行通知より前に発行された C R L と、新たに発行された C R L との差分情報を記載する項目を含む。

【請求項 2 3】

「C R L が発行された」旨を通知する、C R L 発行通知用データフォーマットであって、

新たに失効された証明書の識別情報の一覧を記載する項目を含む。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、公開鍵証明書の失効リストを発行する認証局と、公開鍵証明書の有効性を検証する証明書検証サーバと、上記証明書検証サーバを利用するクライアントと、

からなる認証基盤システムに関する。

【0002】

【従来の技術】

政府認証基盤（以下、GPKI、と記述する）をはじめとして、電子文書の作成者を明らかにし、かつ、当該電子文書が改ざんされていないことを保証するために、公開鍵認証基盤（Public Key Infrastructure、以下、PKI、と記述する）を利用したシステムが普及してきている（例えば、非特許文献1参照）。PKIを利用したシステムでは、電子文書に対して、電子署名を行う者（以下、署名者、と記述する）のみが保有する、秘密鍵（Private key）と呼ばれる鍵によって電子署名が施される。電子署名が施された電子文書を受信した場合には、上記電子署名を検証することで、電子文書の作成者と、当該電子文書が改ざんされていないことと、を確認する。

【0003】

高い信頼が要求される用途では、電子署名の検証を行うためには、上記署名者の公開鍵証明書（以下、証明書、と記述する）に含まれている、公開鍵と呼ばれる鍵によって、当該電子署名を検証するだけでなく、上記署名者の証明書が電子署名を検証する者（以下、検証者、と記述する）にとって有効な証明書であるか否か、を確認する必要がある。上記署名者の証明書が上記検証者にとって有効であるか否か、を検証するには、（1）認証パスの構築と、（2）認証パスの検証と、という、処理が必要である。

【0004】

認証パスとは、上記検証者から上記署名者までの信頼の連鎖であり、証明書のチェーンとして表現される。特に、認証局同士がお互いに証明書を発行しあうような場合には、相互認証証明書という、特殊な証明書を発行する。認証局11から認証局19までの9個の認証局が図2に示したような相互認証の関係を持っている場合には、認証局12が発行した証明書を持つ検証者から認証局11が発行した証明書を持つ署名者までの認証パスは、一番目が相互認証証明書918、二番目が相互認証証明書968、三番目が相互認証証明書946、四番目が相互認証証明書924、最後が検証者の証明書、という順序の証明書チェーンとなる。このようにして構築された検証パスを検証する方法については、上記非特許文献1に詳細に記述されている。

【0005】

また、上記GPKIの仕様書には、証明書の有効性を検証するモデルとして、エンドエンティティモデルと、証明書検証サーバモデルが記載されている。（例えば、非特許文献2参照。）上記証明書検証サーバモデルは、証明書の有効性を検証するために、クライアントに代わってオンラインで証明書の有効性を確認する機能を提供する、証明書検証サーバを利用する。

【0006】

上記証明書検証サーバモデルは、上記エンドエンティティモデルに比べて、次のような利点がある。まず、上記証明書検証サーバモデルでは、上記認証パスを構築する認証パス構築機能をクライアントに実装する必要がないため、クライアントの署名検証プログラムを小さくすることができる。また、クライアントは上記証明書検証サーバの判定結果を信頼するため、上記証明書検証サーバの設定を変更するだけで、システム構成の変化に柔軟に対応できる。上記非特許文献2によれば、証明書が失効されているか否かを判定するには、上記認証局が発行する証明書失効リスト（Certificate Revocation List、以下、CRL、と記述する）やOCSPレスポンドが利用される。

【0007】

検証を行う毎に上記認証局から上記CRLを取得するのは効率が悪い。特許文献1では、上記証明書検証サーバが上記証明書や上記CRLや上記検証パスをキャッシュすることにより証明書の有効性判定処理を高速化する方式が開示されている。

【0008】

ところで、電子署名を検証したり、検証パスを構築したりするためには、署名者の証明書を入手することが必要である。署名者の証明書を入手する方法は大きく二つに分類することができる。

【0009】

一つは、署名者からは電子署名付き電子文書が送付されるのみであり、当該署名者の証明書は別途入手する、という方法である。例えば、電子署名付き電子文書とともに、当該電子署名を検証するための証明書が格納されている場所を示すURLを通知する方法などが該当する。この方法では、上記検証者は、上記証明書が格納された場所（以下、証明書リポジトリ、と記述する）などにアクセスし、当該証明書を入手する必要がある。もう一つは、署名者が、電子署名付き電子文書とともに、当該電子署名を検証するために利用する証明書を添付して送付する、という方法である。

【0010】

【特許文献1】

特開2002-72876号公報

【非特許文献1】

ITU、ITU-T Recommendation X.509 “Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks”、ITU、2000年3月、p. 7-53

【非特許文献2】

「政府認証基盤（GPKI） 政府認証基盤相互運用性

仕様書」p. 18-20, 27-29、[online]、平成13年4月25日、基本問題専門部会了承、[2003年3月14日検索]、インターネット<URL: http://www.soumu.go.jp/gyoukan/kanri/010514_2.pdf>

【0011】

【発明が解決しようとする課題】

証明書の有効性判定処理を高速化するために上記CRLをキャッシュすると、上記認証局が上記CRLを緊急に発行した場合に、キャッシュしている上記CRLが最新のものではなくなる。特許文献1にはこの点について言及していない。

【0012】

上記の課題を解決する方法の一つとしては、上記CRLが緊急発行された場合にも有効性検証が正しく行われるために、上記証明書検証サーバが、上記CRLの格納場所（以下、CRLリポジトリと呼ぶ）に定期的にアクセスし、上記CRLが更新されていないかを確認する方法がある。上記方法は、さらに、上記証明書検証サーバ自身がネットワークを介して確認を行う方式と、上記CRLリポジトリにCRL発行確認ソフトウェアを導入して確認を行う方式と、の2種類がある。

【0013】

上記CRLが更新されていないかを定期的に確認する方法を利用して、上記証明書の有効性検証結果の精度を高めるためには、上記確認の間隔をできる限り短くすることが必要である。しかし、上記証明書検証サーバ自身がネットワークを介して確認を行う方式では、上記確認の間隔を短くするとネットワークの負荷が大きくなる、という課題がある。

【0014】

一方、上記CRLリポジトリに確認を行うためのCRL発行確認ソフトウェアを導入する方式の場合には、上記CRLリポジトリの運営者と上記証明書検証サーバの運営者とが異なると、上記CRL発行確認ソフトウェアのインストールが許可されず、上記確認が行えない場合がある、という課題がある。

【0015】

また、複数の上記証明書検証サーバが存在する環境では、すべての上記証明書検証サーバが上記CRLリポジトリに導入された上記CRL発行確認ソフトウェアを利用しなければ、すべての上記証明書検証サーバが同じ精度で証明書有効性検証を行うことができないため、稼働している上記証明書検証サーバの数を増減させたい場合には、上記CRL発行確認ソフトウェアの設定を変更する必要があるが、上記CRLリポジトリの運営者と上記証明書検証サーバの運営者とが異なると、上記証明書検証サーバの数を柔軟に変更することが困難である、という課題がある。

【0016】

さらに、上記検証パスをキャッシュしているとしても、上記認証局によって古い相互認証証明書が破棄され、新しい相互認証証明書が発行されていた場合には、新しい相互認証証明書を含む検証パスを構築する必要がある。

【0017】

また、複数の上記証明書検証サーバが存在する環境では、複数の上記証明書検証サーバが、同じ上記証明書の有効性を検証した場合でも、各々の上記証明書検証サーバが上記認証パスの構築や、上記CRLの取得などを行うため、特定の上記CRLリポジトリや上記証明書リポジトリにアクセスが集中したり、ネットワークの負荷が大きくなったりする可能性がある。特許文献1にはこれらについて言及していない。

【0018】

また、上記証明書を別途入手する方法では、上記クライアントは、上記証明書検証サーバに上記証明書の有効性検証を依頼するため、まず、上記証明書リポジトリにアクセスして上記証明書を取得しなければならない、という課題がある。

【0019】

従って、上記各課題を解決する新たな手法が求められている。

【0020】

【課題を解決するための手段】

本発明は、上記証明書を発行する証明書発行手段と、上記CRLを発行するCRL発行手段と、を備えた認証局と、上記認証局が発行した上記証明書を格納する証明書格納手段を備えた証明書リポジトリと、上記認証局が発行した上記CRLを格納するCRL格納手段を備えたCRLリポジトリと、上記証明書の有効性を検証する証明書有効性検証手段と、上記CRLリポジトリから取得した上記CRLをキャッシュするCRLキャッシュ手段と、上記証明書有効性検証手段が上記証明書の有効性を検証するために構築した検証パスをキャッシュする検証パスキャッシュ手段と、を備えた証明書検証サーバと、電子署名を検証する電子署名検証手段と、上記証明書検証サーバに上記証明書の有効性検証を依頼する証明書有効性検証依頼手段と、を備えたクライアントと、から構成される、認証基盤システムにおいて、上記認証局に、上記CRLを発行すると同時に、上記証明書検証サーバに「上記CRLが発行された」旨を通知する、CRL発行通知を送信する、CRL発行通知送信手段、を設け、上記証明書検証サーバに、上記認証局から上記CRL発行通知を受信する、CRL発行通知受信手段、を設けたことを特徴とする。

【0021】

また、本発明は、上記証明書検証サーバの上記CRLキャッシュ手段は、上記CRL発行通知受信手段によって、上記CRL発行通知を受信した場合に、上記認証局

が新たに発行した上記CRLを上記CRLリポジトリから取得するものであること、を特徴とする。

【0022】

さらに、本発明は、上記証明書検証サーバに、上記CRLが新たに発行されたことを発見した場合に、予め登録された、他の証明書検証サーバに対して、「CRLが発行された」旨を通知する、CRL発行通知送信手段、を設けたことを特徴とする。

【0023】

また、本発明は、上記認証局に、上記証明書発行手段によって上記証明書が発行された場合に、上記証明書検証サーバに「証明書が発行された」旨を通知する証明書発行通知を送信する、証明書発行通知送信手段を設け、前記証明書検証サーバに、上記証明書発行通知を受信する、証明書発行通知受信手段を設け、上記証明書有効性検証手段は、上記証明書発行通知受信手段が上記証明書発行通知を受信した場合に、新たに発行された上記証明書を含むような、上記検証パスを作成するものであって、上記検証パスキャッシュ手段は当該検証パスをキャッシュするものであること、を特徴とする。

【0024】

さらに、本発明は、上記証明書検証サーバに、上記検証パスを構築した場合に、予め登録された、他の証明書検証サーバに当該検証パスを送信する、検証パス送信手段を設け、上記検証パスキャッシュ手段は、他の証明書検証サーバから上記検証パスを受信した場合に、当該検証パスをキャッシュするものであること、を特徴とする。

【0025】

さらに、本発明は、上記クライアントは、上記電子署名を検証するために必要な、上記証明書の取得を、上記証明書検証サーバに依頼する、証明書取得依頼手段、を設け、上記証明書検証サーバに、上記クライアントから取得を要求された上記証明書を上記証明書リポジトリから取得し、かつ、上記証明書検証手段によって、当該証明書が有効であると判定された場合に、上記クライアントに当該証明書を送信する、証明書取得手段、を設けたことを特徴とする。

【0026】

さらに、本発明は、「上記CRL発行通知の送信を依頼する」旨のメッセージを作成する手段を上記証明書検証サーバに設け、上記CRL発行通知依頼メッセージを受信する手段を上記認証局に設け、さらに、上記認証局の上記CRL発行通知送信手段は、当該認証局に対して上記CRL発行通知依頼メッセージを送信してきた証明書検証サーバに対して、上記CRL発行通知を送信することを特徴とする。

【0027】

また、本発明は、上記CRLリポジトリに新たなCRLが格納されたことを発見した場合に、「CRLが発行された」旨のCRL発行通知を送信するCRL発行通知送

信手段と、「上記CRL発行通知の送信を依頼する」旨のCRL発行通知依頼メッセージを受信するCRL発行通知依頼受信手段とを、上記CRLリポジトリに備えたことを特徴とする。

【0028】

また、本発明のCRL発行確認ソフトウェアは、CRLの発行を監視し、新たなCRLの発行された場合に、CRL発行通知を送信する手段を実現するものであり、CRL発行通知依頼メッセージを受信する手段を実現し、上記CRL発行通知送信手段は、上記CRL発行通知を受信した上記CRL発行通知依頼メッセージの送信元に送信することを特徴とする。

【0029】

さらに、本発明の上記証明書検証サーバは、前記CRL発行通知依頼作成手段によって作成されたCRL発行通知依頼メッセージを受信する手段を設けたことを特徴とする。

【0030】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態について説明する。なお、これによって本発明が限定されるものではない。

【0031】

図1は、本発明の実施例である電子署名付き電子文書交換システムの一構成を示した図である。認証局1₁から認証局1₉までの9個の認証局（以下、まとめて、認証局1、と記述する）と、証明書リポジトリ2と、CRLリポジトリ3と、証明書検証サーバ4₁から証明書検証サーバ4_nまでのn個の証明書検証サーバ（以下、まとめて、証明書検証サーバ4、と記述する）と、上記証明書検証サーバ4に証明書の有効性の検証を依頼する、クライアント端末5₁からクライアント端末5_mまでのm個のクライアント端末（以下、まとめて、クライアント端末5、と記述する）と、がネットワーク0を介して接続されている。

【0032】

上記認証局1は、上記クライアント端末5に証明書509を発行し、かつ、当該証明書509のコピーを上記証明書リポジトリ2に格納する証明書発行機能101と、失効した上記証明書509のリストであるCRL7を発行し、かつ、当該CRL7を上記CRLリポジトリに格納するCRL発行機能102と、上記CRL7が発行されたことを通知するCRL発行通知8を、上記証明書検証サーバ4に対して送信する、CRL発行通知機能103と、「上記CRL発行通知8の送信を依頼する」旨の、CRL発行通知依頼メッセージ10を受信するCRL発行通知依頼受信機能105と、を備えている。

【0033】

また、認証局1₁から認証局1₉までの、上記認証局1は、相互認証証明書9を発行しあい、図2に示したよう

な、相互認証の関係がある。

【0034】

上記証明書リポジトリ2は、上記証明書509を保持する、証明書DB201と、上記認証局1から上記証明書509を受信し、かつ、当該証明書509を上記証明書DB201に格納し、さらには、指定された上記証明書509を上記証明書DB201から検索して返信する、証明書DB管理機能202と、を備えている。

【0035】

上記CRLリポジトリ3は、上記CRL7を保持する、CRLDB301と、上記認証局1から上記CRL7を受信し、かつ、当該CRLを上記CRLDB301に格納し、さらには、指定された上記CRL7を上記CRLDB301から検索して返信する、証明書DB管理機能302と、を備えている。

【0036】

上記証明書検証サーバ4は、
上記CRL7をキャッシュしたCRLキャッシュ401と、
上記証明書509の有効性を検証するために使用する、
検証パスをキャッシュした検証パスキャッシュ402と、

上記クライアント端末5からの要求を受けて、証明書の有効性を検証する証明書検証機能403と、

上記クライアント端末5からの要求を受けて、上記証明書リポジトリ2から上記証明書509を取得し、かつ、当該証明書509の有効性を上記証明書検証機能403によって検証し、さらには、当該証明書509が有効であった場合に上記クライアント端末5に返信する、証明書取得機能404と、

上記CRLリポジトリ3から上記CRL7を取得し、かつ、当該CRL7を上記CRLキャッシュ401に格納する、CRL管理機能405と、

上記認証局1から上記CRL発行通知8を受信し、かつ、上記認証局1から上記CRL発行通知8を受け取った場合に、予め登録された、あるいは、上記CRL発行通知依頼メッセージ10を送信することにより当該CRL発行通知8の転送を依頼してきた、他の証明書検証サーバ4に当該CRL発行通知8を転送する、CRL発行通知管理機能406と、

上記証明書検証機能403が作成した上記検証パスを上記検証パスキャッシュ402にキャッシュし、かつ、当該検証パスを予め登録された他の証明書検証サーバ4に対して送信し、さらには、他の証明書検証サーバ4から受信した上記検証パスを上記検証パスキャッシュ402にキャッシュする、検証パス管理機能407と、

上記認証局1に対して上記CRL発行通知8の送信を依頼する、CRL発行通知依頼メッセージ10を作成する、CRL発行通知依頼作成機能410と、

他の証明書検証サーバ4から上記CRL発行通知依頼メ

ッセージ10を受信する、CRL発行通知依頼受信機能411と、を備えている。

【0037】

上記クライアント端末5は、
他のクライアント端末5と電子文書6を交換する、電子文書交換機能501と、
上記電子文書6に電子署名を行い、かつ、他のクライアント端末5から受信した上記電子文書6に行われた電子署名を検証する、電子署名機能502と、

10 上記証明書検証サーバ4に上記証明書509の有効性の検証を要求し、かつ、上記証明書検証サーバ4から上記証明書509の有効性検証の結果を受信する、証明書検証要求機能503と、

上記電子文書6に上記証明書509ではなく、上記証明書509の格納場所を示したURLが添付されていた場合に、当該URLに格納されている上記証明書509を取得するために上記証明書検証サーバ4に当該証明書識別情報を送信し、かつ、上記証明書検証サーバ4から当該証明書509を受信する、証明書取得依頼機能506と、

20 と、
上記電子署名作成機能502が利用する、秘密鍵508と、

上記認証局1が発行した、上記証明書509と、を備えている。

【0038】

なお、上記クライアント端末51の上記証明書5091は上記認証局11から発行されており、上記クライアント端末52の上記証明書5092は上記認証局12から発行されている。

30 【0039】

また、本実施例では、上記証明書検証要求機能503と、上記証明書取得依頼機能506と、が利用する上記証明書検証サーバ4は、上記証明書検証サーバ41から上記証明書検証サーバ4nまでの上記証明書検証サーバ4のうち、予め定められた、特定の上記証明書検証サーバ4を利用する。

【0040】

例えば、クライアント端末52は上記証明書検証サーバ41を利用する。

40 【0041】

なお、図1に示す認証局1、証明書リポジトリ2、CRLリポジトリ3、証明書検証サーバ4、クライアント端末5、の各装置は、例えば、図9に示すような、CPU91と、メモリ92と、ハードディスク等の外部記憶装置93と、CD-ROM等の可搬性を有する記憶媒体99から情報を読み取る読取装置94と、ネットワークを介して他装置と通信を行うための通信装置95と、キーボードやマウス等の入力装置96と、モニタやプリンタ等の出力装置97と、これらの各装置間のデータ送受を行うインターフェース98とを備えた、一般的な電子計

算機において、CPU91がメモリ92上にロードされた所定のプログラムを実行することにより、実現できる。

【0042】

すなわち、証明書発行機能101、CRL発行機能102、CRL発行通知機能103、CRL発行通知依頼受信機能105、証明書DB管理機能202、CRLDB管理機能302、証明書検証機能403、証明書取得機能404、CRL管理機能405、CRL発行通知管理機能406、検証パス管理機能407、CRL発行通知依頼作成機能410、CRL発行通知依頼受信機能411、電子文書交換機能501、電子署名機能502、証明書検証要求機能503、証明書取得依頼機能504、はCPU91が所定のプログラムを実行することによるプロセスとして実現できる。また、証明書DB201、CRLDB301、CRLキャッシュ401、検証パスキャッシュ402、は、CPU91がメモリ92や外部記憶装置63を利用することにより実現できる。

【0043】

このような電子計算機上に、上記各装置を実現するための所定のプログラムは、読取装置94を介して電子計算機が利用可能な記憶媒体99から導入されてもよいし、あるいは、通信装置96を介してネットワークまたはネットワークを伝搬する搬送波といった、電子計算機が利用可能な通信媒体を介して他のサーバから導入されてもよい。

【0044】

導入に際しては、一旦、外部記憶装置93に格納された後、そこからメモリ92上にロードされてCPU91に実行されてもよいし、あるいは、外部記憶装置93に格納されることなく、直接メモリ92上にロードされて、CPU91に実行されてもよい。

【0045】

次に、図1の電子署名利用システムの動作について、上記証明書検証サーバ4が上記認証局1に対して上記CRL発行通知8の送信を依頼する場合の動作について、図面を用いて説明する。

【0046】

図7は、図1の電子署名利用システムにおいて、上記証明書検証サーバ4が上記認証局1に対して上記CRL発行通知8の送信を依頼する場合の、上記証明書検証サーバ4と、上記認証局1と、の動作を示す。

【0047】

上記証明書検証サーバ4において、上記CRL発行通知依頼作成機能410が、上記CRL発行通知依頼メッセージ10を作成し（ステップ7101）、上記認証局1に送信する（ステップ7102）。

【0048】

図8（a）に例示する、CRL発行通知依頼メッセージ10は、「上記CRL発行通知8の送信を依頼する」旨

のメッセージと、上記CRL発行通知8の送信先となるネットワーク0上のアドレスであるホスト名と、から構成されている。

【0049】

上記認証局1では、上記CRL発行通知依頼受信機能105が、上記CRL発行通知依頼メッセージ10を受信する（ステップ7201）と、当該CRL発行通知依頼メッセージ10を送信してきた、上記証明書検証サーバ4のホスト名をCRL発行通知送信先リスト104に追加する（ステップ7202）。

【0050】

上記証明書検証サーバ4₁から上記証明書検証サーバ4₂への上記CRL発行通知8の転送を依頼する場合には、まず、上記証明書検証サーバ4₁の上記CRL発行通知依頼作成機能410が上記CRL発行通知依頼メッセージ10を作成し、上記証明書検証サーバ4₂に送信する。

【0051】

上記証明書検証サーバ4₂のCRL発行通知依頼受信機能411は、当該CRL発行通知依頼メッセージ10を受信し、送信元である上記証明書検証サーバ4のホスト名をCRL発行通知転送先リスト408に追加する。

【0052】

上記証明書検証サーバ4が上記認証局1に対して上記CRL発行通知8の送信停止を依頼する場合には、図8（b）に例示するような、CRL発行通知依頼メッセージ10を、上記認証局1に送信する。

【0053】

図8（b）のCRL発行通知依頼メッセージ10は、「上記CRL発行通知8の送信停止を依頼する」旨のメッセージと、上記CRL発行通知8の送信先のホスト名と、から構成されている。

【0054】

上記認証局1は、図8（b）のCRL発行通知依頼メッセージ10を受信したら、記載されている上記証明書検証サーバ4のホスト名をCRL発行通知転送先リスト408から削除する。

【0055】

上記証明書検証サーバ4が、他の証明書検証サーバ4に上記CRL発行通知8の転送を依頼したり、転送停止を依頼したりする場合には、依頼先の証明書検証サーバ4に、上記CRL発行通知依頼メッセージ10を送信する。

【0056】

次に、図1の電子署名利用システムにおいて、上記CRL7が発行された場合の、上記認証局1と、上記CRLリポジトリ3と、上記証明書検証サーバ4と、の動作について、図面を用いて説明する。

【0057】

図3は、図1の電子署名利用システムにおいて、上記C

R L 7が発行された場合の、上記認証局 1 と、上記 C R L リポジトリ 3 と、上記証明書検証サーバ 4 と、の動作を示す図である。

【0058】

まず、上記認証局 1 の動作について説明する。

【0059】

上記認証局 1 は、上記 C R L 発行機能 102 が上記 C R L 7 を作成する（ステップ 3101）と、当該 C R L 発行機能 102 が当該 C R L 7 を上記 C R L リポジトリ 3 に送信する（ステップ 3102）。

【0060】

次に、上記 C R L 発行通知機能 103 が、上記 C R L 発行通知 8 を作成し、予め定められた、あるいは、上記 C R L 発行通知依頼メッセージ 10 を送信することにより当該 C R L 発行通知 8 の送信を依頼してきた、上記証明書検証サーバ 4 に送信する（ステップ 3103）。

【0061】

なお、本実施例では、認証局 1 は、C R L 発行通知送信先リスト 104 にホスト名が記載されている、上記証明書検証サーバ 4 に上記 C R L 発行通知 8 を送信する。

【0062】

図 6 の（a）は、上記認証局 1 が管理している C R L 発行通知送信先リスト 104 の一例であり、上記証明書検証サーバ 4₁ のホスト名と、上記証明書検証サーバ 4_n のホスト名と、が記載されている。

【0063】

したがって、上記認証局 1 の上記 C R L 発行通知機能 103 は、上記証明書検証サーバ 4₁ と、上記証明書検証サーバ 4_n と、に上記 C R L 発行通知 8 を送信する。

【0064】

次に、上記 C R L リポジトリ 3 の動作について説明する。

【0065】

上記 C R L リポジトリ 3 の上記 C R L DB 管理機能 302 は、上記認証局 1、あるいは、上記証明書検証サーバ 4 からのアクセスを待ち受け、上記認証局 1 から上記 C R L 7 を受信する（ステップ 3301）と、当該 C R L 7 を上記 C R L DB 301 格納し（ステップ 3302）、再び、上記認証局 1、あるいは、上記証明書検証サーバ 4 からのアクセスを待ち受ける。

【0066】

一方、上記証明書検証サーバ 4 から、上記 C R L 7 を送信するように依頼を受ける（ステップ 3303）と、上記 C R L DB 301 から当該 C R L 7 を検索し（ステップ 3304）、上記証明書検証サーバ 4 に当該 C R L 7 を送信して（ステップ 3305）、再び、上記認証局 1、あるいは、上記証明書検証サーバ 4 からのアクセスを待ち受ける。

【0067】

次に、上記証明書検証サーバ 4 の動作について説明す

る。

【0068】

ここでは、上記認証局 1 から上記 C R L 発行通知 8 を受信する上記証明書検証サーバ 4₁ の動作によって、上記証明書検証サーバ 4 の動作を説明する。

【0069】

まず、上記証明書検証サーバ 4₁ では、上記 C R L 発行通知管理機能 406 が、上記認証局 1、あるいは、他の証明書検証サーバ 4、から上記 C R L 発行通知 8 を受信する（ステップ 3401）と、まず、当該 C R L 発行通知 8 を既に受信したかどうかを調べ（ステップ 3402）、当該 C R L 発行通知 8 を既に受信していた場合には、そのまま処理を終了する。

【0070】

一方、上記 C R L 発行通知 8 を初めて受信した場合には、上記 C R L 管理機能 405 が、上記 C R L リポジトリ 3 にアクセスし（ステップ 3403）、上記 C R L 7 を取得し（ステップ 3404）、上記 C R L キャッシュ 401 キャッシュする（ステップ 3405）。

【0071】

次に、上記 C R L 発行通知管理機能 406 は、予め登録された、あるいは、上記 C R L 発行通知依頼メッセージ 10 を送信することにより当該 C R L 発行通知 8 の転送を依頼してきた、他の証明書検証サーバ 4 に、上記 C R L 発行通知 8 を転送する（ステップ 3406）。

【0072】

上記証明書検証サーバ 4 は、C R L 発行通知転送先リスト 408 というリストを利用して、上記 C R L 発行通知 6 を転送する、上記証明書検証サーバ 4 を管理している。

【0073】

図 6 の（b）は、上記証明書検証サーバ 4₁ が管理している上記 C R L 発行通知転送先リスト 408 の一例であり、上記証明書検証サーバ 4₂ のホスト名と、上記証明書検証サーバ 4₃ のホスト名と、上記証明書検証サーバ 4_n のホスト名とが記載されている。

【0074】

したがって、上記 C R L 発行通知管理機能 406 は、上記 C R L 発行通知 6 を、上記証明書検証サーバ 4₂ と、上記証明書検証サーバ 4₃ と、上記証明書検証サーバ 4_n に転送する。

【0075】

なお、本実施例では、上記証明書検証サーバ 4₁ から上記証明書検証サーバ 4_n までの各々のホスト名は、上記証明書検証サーバ 4₁ から上記証明書検証サーバ 4_n までの証明書検証サーバ 4 が各々に保持している、上記 C R L 発行通知転送先リスト 408 のいずれかに必ず記載されているようにしている。

【0076】

こうすることにより、どれか一つの上記証明書検証サー

サーバ4が上記認証局1から上記CRL発行通知6を受け取れば、上記証明書検証サーバ4₁から上記証明書検証サーバ4_nまでのすべての証明書検証サーバ4が上記CRL発行通知6を受け取ることができる。

【0077】

また、上記証明書検証サーバ4を新たに追加する場合には、上記証明書検証サーバ4₁から上記証明書検証サーバ4_nまでの証明書検証サーバ4が各々に保持している、上記CRL発行通知転送先リスト408のいずれかに当該証明書検証サーバ4のホスト名を追加すれば、上記CRL発行通知送信先リスト104を変更する必要はなくなる。

【0078】

以上が、上記CRL7が発行された場合の、図1の電子署名利用システムの動作である。

【0079】

次に、図1の電子署名付き電子文書交換システムにおいて、上記クライアント端末5₁から、上記クライアント端末5₂に、上記電子文書6を送信する場合の動作について、図面を用いて説明する。

【0080】

なお、本実施例では、上記電子文書6に施された電子署名を検証するための上記証明書509は、上記電子文書6に添付される場合と、上記電子文書6に添付されない場合と、の二つの場合があるが、まずは、上記電子文書6に施された電子署名を検証するための上記証明書509が、上記電子文書6に添付される場合について説明する。

【0081】

図4は、図1の電子署名付き電子文書交換システムにおいて、上記電子文書6に施された電子署名を検証するための上記証明書509が、上記電子文書6に添付される場合に、上記クライアント端末5₁から、上記クライアント端末5₂に、上記電子文書6を送信する際の、上記クライアント端末5₁と、上記クライアント端末5₂と、上記証明書検証サーバ4₁と、上記証明書検証サーバ4₂と、の動作を示した図である。

【0082】

まず、上記クライアント端末5₁の動作について説明する。

【0083】

上記クライアント端末5₁は、上記電子文書交換機能501が、上記クライアント端末5₂に送信する、上記電子文書6を作成する（ステップ4501）と、上記電子署名機能502が、上記秘密鍵508₁を使用して、当該電子文書6に電子署名を施す（ステップ4502）。

【0084】

次に、上記電子文書交換機能501は、電子署名が施された、上記電子文書6を、上記証明書509₁とともに、上記クライアント端末5₂に送信する（ステップ4

503）。

【0085】

次に、上記クライアント端末5₂の動作について説明する。

【0086】

上記クライアント端末5₂は、上記電子文書6を受信する（ステップ4511）と、上記電子文書6とともに送信されてきた上記証明書509₁の有効性を検証するため、上記証明書有効性確認機能503が、上記証明書検証サーバ4₁に当該証明書509₁の有効性検証を依頼し（ステップ4512）、上記証明書検証サーバ4₁から有効性検証の結果を受信する（ステップ4513）。

【0087】

ここで、上記有効性検証の結果が、上記証明書509₁は、上記クライアント端末5₂にとって有効ではない、というものであった場合、処理を終了する。

【0088】

一方、上記有効性検証の結果が、上記証明書509₁は、上記クライアント端末5₂にとって有効である、というものであった場合、上記電子署名機能503は、上記証明書509₁から公開鍵を取り出し、上記電子文書6に施されている電子署名を検証する（ステップ4515）。ここで、上記電子署名が正しくないと判定された場合には処理を終了する。

【0089】

一方、上記電子署名が正しいと判定された場合には、上記電子署名6を保存する（ステップ4516）。

【0090】

次に、上記証明書検証サーバ4の動作について説明する。

【0091】

まず、上記証明書検証サーバ4₁は、上記クライアント端末5₂から上記証明書509₁の有効性検証を依頼される（ステップ4401）と、上記証明書検証機能403が、上記クライアント端末5₂から上記クライアント端末5₁までの検証パスが、上記検証パスキャッシュ402に存在しているかを確認する（ステップ4402）。

【0092】

ここで、上記検証パスキャッシュ402に、当該検証パスが存在する場合には、ステップ4404に進む。一方、上記検証パスキャッシュ402に、当該検証パスが存在しなかった場合には、当該検証パスを構築し（ステップ4403）、ステップ4404に進む。

【0093】

ステップ4404では、上記証明書検証403は、上記CRLキャッシュ401から上記CRL7を取り出し、上記検証パスが有効か否かを判定する。次に、判定結果を上記クライアント端末5₂に送信する（ステップ4405）。

【0094】

ここで、上記検証パスが、ステップ4403で新たに構築されたものでない場合には、処理を終了する。一方、上記検証パスが、ステップ4403で新たに構築されたものであった場合には、検証パス送信先リスト409にホスト名が記載されている、上記証明書検証サーバ4に当該検証パスを送信し（ステップ4407）、処理を終了する。

【0095】

上記検証パス送信先リスト409は、新たに構築した上記検証パスを送信する上記証明書検証サーバ4のホスト名を記載したリストであり、本実施例では、上記CRL発行通知転送先リスト408を上記検証パス送信先リスト409にも利用している。

【0096】

したがって、ステップ4407では、上記検証パスは、上記証明書検証サーバ4₂と、上記証明書検証サーバ4₃と、上記証明書検証サーバ4_nと、に送信される。

【0097】

なお、本実施例では、上記CRL発行通知転送先リスト408と、上記検証パス送信先リスト409と、に同じリストを使用しているが、本発明はそれに限定されるものではなく、個々に異なるリストを利用しても良い。

【0098】

一方、上記証明書検証サーバ4₂や、上記証明書検証サーバ4₃や、上記証明書検証サーバ4_nは、上記証明書検証サーバ4₁から上記検証パスを受信する（ステップ4411）と、上記検証パス管理機能407は当該検証パスが上記検証パスキャッシュ402にキャッシュされているかどうかを確認する（ステップ4412）。

【0099】

ここで、上記検証パスキャッシュ402に上記検証パスがキャッシュされていれば、何もせず、処理を終了する。一方、上記検証パスキャッシュ402に上記検証パスがキャッシュされていなければ、当該検証パスを上記検証パスキャッシュ402にキャッシュし（ステップ4413）、検証パス送信先リスト409にホスト名が記載されている、上記証明書検証サーバ4に当該検証パスを送信し（ステップ4414）、処理を終了する。

【0100】

なお、本実施例では、上記証明書検証サーバ4の上記検証パス管理機能407は、検証パスを送受したり、キャッシュしたりするようにしているが、本発明はそれに限定されるものではなく、上記検証パスを一意に識別できるような検証パス情報を送受したり、キャッシュしたりし、必要なときに当該検証パス情報から対応する検証パスを構成するようにしてもよい。

【0101】

以上が、上記電子文書6に施された電子署名を検証するための上記証明書509が上記電子文書6に添付される

場合の、上記クライアント端末5₁から上記クライアント端末5₂に上記電子文書6を送信する際の、図1の電子署名付き電子文書交換システムの動作である。

【0102】

次に、上記電子文書6に施された電子署名を検証するための上記証明書509が上記電子文書6に添付されない場合の、上記クライアント端末5₁から上記クライアント端末5₂に上記電子文書6を送信する際の、図1の電子署名付き電子文書交換システムの動作について、図面を用いて説明する。

【0103】

図5は、図1の電子署名付き電子文書交換システムにおいて、上記電子文書6に施された電子署名を検証するための上記証明書509が、上記電子文書6に添付されない場合に、上記クライアント端末5₁から上記クライアント端末5₂に上記電子文書6を送信する際の、上記クライアント端末5₁と、上記クライアント端末5₂と、上記証明書検証サーバ4と、上記証明書リポジトリ2と、の動作を示した図である。

【0104】

まず、上記クライアント端末5₁の動作について説明する。

【0105】

上記クライアント端末5₁は、上記電子文書交換機能501が、上記クライアント端末5₂に送信する、上記電子文書6を作成する（ステップ5501）と、上記電子署名機能502が、上記秘密鍵508₁を使用して、当該電子文書6に電子署名を施す（ステップ5502）。

【0106】

次に、上記電子文書交換機能501は、電子署名が施された、上記電子文書6を、上記証明書509₁の格納場所を示したURLとともに、上記クライアント端末5₂に送信する（ステップ5503）。

【0107】

なお、本実施例では、上記電子文書6とともに、上記証明書509の格納場所を示したURLを送信するようにしているが、本発明はこれに限定されるものではなく、上記証明書509に記載されている情報の一部を送信するようにしてもよい。

【0108】

次に、上記クライアント端末5₂の動作について説明する。

【0109】

上記クライアント端末5₂は、上記電子文書6を受信する（ステップ5511）と、上記証明書取得依頼機能504が、上記電子文書6とともに送信されてきた上記URLに対応する上記証明書509₁を上記証明書検証サーバ4₁に取得するように依頼し（ステップ5512）、上記証明書検証サーバ4₁から依頼結果を受信する（ステップ5513）。

【0110】

ここで、上記依頼結果に上記証明書5091が含まれていなかった場合、すなわち、上記URLが示す上記証明書5091が上記クライアント端末52にとって有効なものでない、と上記証明書検証サーバ41が判断した場合には、処理を終了する。一方、上記依頼結果に上記証明書5091が含まれていた場合、上記電子署名機能503は、上記証明書5091から公開鍵を取り出し、上記電子文書6に施されている電子署名を検証する（ステップ5515）。ここで、上記電子署名が正しくないと判定された場合には、処理を終了する。一方、上記電子署名が正しいと判定された場合には、上記電子署名6を保存し（ステップ5516）、処理を終了する。

【0111】

次に、上記証明書検証サーバ4の動作について説明する。

【0112】

上記証明書検証サーバ41の上記証明書取得機能404は、上記クライアント端末52から、上記証明書5091を取得するように依頼を受けると（ステップ5401）、上記クライアント端末52から送信された上記URLを用いて、上記証明書リポジトリ2にアクセスし（ステップ5402）、上記証明書5091を取得する（ステップ5403）。

【0113】

次に、上記証明書検証機能403によって、上記証明書5091が、上記クライアント端末52にとって、有効な証明書であるか否かを判定する（ステップ5404）。

【0114】

ここで、上記証明書検証機能403の動作については、図4のステップ4402からステップ4409までの動作と同じであり、説明を省略する。

【0115】

上記判定によって、上記証明書5091が、上記クライアント端末52にとって、有効な証明書である、と判定された場合、当該証明書5091を含む依頼結果を作成し（ステップ5405）、上記クライアント端末52に送信する（ステップ5407）。一方、上記証明書5091が、上記クライアント端末52にとって、有効な証明書でない、と判定された場合には、「有効でない」旨を示す依頼結果を作成し（ステップ5406）として上記クライアント端末52に送信する（ステップ5407）。

【0116】

次に、上記証明書リポジトリ2の動作について説明する。

【0117】

上記証明書リポジトリ2の上記証明書DB管理機能202は、上記証明書検証サーバ41から、上記証明書50

91を送信するように依頼を受ける（ステップ5201）と、上記証明書DB201から当該証明書5091を検索し（ステップ5202）、上記証明書検証サーバ4に当該証明書5091を送信する（ステップ5203）。

【0118】

以上が、上記電子文書6に施された電子署名を検証するための上記証明書509が上記電子文書6に添付されない場合の、上記クライアント端末51から上記クライアント端末52に上記電子文書6を送信する際の、図1の電子署名付き電子文書交換システムの動作である。

【0119】

このように、本実施例の電子署名付き電子文書交換システムでは、上記認証局1が上記CRL7を発行する際に、上記CRL発行通知8を、上記CRL発行通知送信先リスト104にホスト名が記載された、上記証明書検証サーバ4に送信することで、上記CRL7を発行したことを上記証明書検証サーバ4に通知し、かつ、上記CRL発行通知8を受信した上記証明書検証サーバ4は、上記CRLリポジトリ3から上記CRL7を取得して、キャッシュするようにしている。

【0120】

このため、上記認証局1が上記CRL7を緊急に発行したような場合でも、上記証明書検証サーバ4がキャッシュしているCRLは最新のものであるため、上記証明書509の有効性検証結果の精度を保証することができる。

【0121】

また、本実施例の電子署名付き電子文書交換システムでは、上記CRL発行通知8を受信した上記証明書検証サーバ4は、上記CRL発行通知転送先リスト408にホスト名が記載されている、他の証明書検証サーバ4に、当該CRL発行通知8を転送するようにしている。

【0122】

このため、新しく証明書検証サーバ4を追加するような場合でも、上記証明書検証サーバ4の上記CRL発行通知転送先リスト408に、新たな証明書検証サーバ4のホスト名を記載するだけで、上記CRL発行通知8を受信することができるようになり、上記認証局1側の設定を変更する必要はない。

【0123】

また、本実施例の電子署名付き電子文書交換システムでは、上記証明書検証サーバ4が、他の証明書検証サーバ4から上記検証パスを受信した場合に、当該検証パスをキャッシュし、かつ、上記証明書検証サーバ4が新たに検証パスを構築した場合には、上記検証パス送信先リスト409にホスト名が記載されている、他の証明書検証サーバ4に、当該新たな検証パスを送信するようにしている。

【0124】

このため、複数の上記証明書検証サーバ 4 の間で検証パスを共有することができるため、上記証明書リポジトリ 2 や上記 C R L リポジトリ 3 へのアクセスが集中したり、ネットワークの負荷が増大することを防ぐことができる。

【0125】

さらに、本実施例の電子署名付き電子文書交換システムでは、上記クライアント端末 5 が、上記証明書 509 の格納場所を示した URL を受信した場合に、上記証明書リポジトリ 2 にアクセスするのではなく、上記証明書検証サーバ 4 に上記証明書 509 の取得を依頼し、かつ、上記証明書検証サーバ 4 は、上記証明書リポジトリ 2 から取得した上記証明書 509 が、上記クライアント端末 5 にとって有効な証明書であった場合にのみ、上記証明書 509 を上記クライアント端末 5 に返信するようにしている。

【0126】

このため、上記クライアント端末 5 には、上記証明書リポジトリ 2 にアクセスする機能を実装する必要がない。

【0127】

なお、本実施例では、上記 C R L 発行通知 8 には、「C R L が発行された旨」の通知のみが記載されているが、本発明はそれに限定されるものではない。

【0128】

例えば、上記 C R L 発行通知 8 には、新たに発行された上記 C R L 7 自身が含まれていたり、あるいは、以前に発行された C R L 7 と、新たに発行された C R L 7 との、差分情報が含まれていたりしてもよい。さらには、新たに失効された証明書 509 の識別情報の一覧が含まれていてもよい。

【0129】

上記 C R L 発行通知 8 に、新たに発行された上記 C R L 7 自身や、以前に発行された C R L 7 と新たに発行された C R L 7 との差分情報や、新たに失効された証明書 509 の識別情報の一覧を含めることにより、当該 C R L 発行通知 8 を受信した上記証明書検証サーバ 4 は、上記 C R L リポジトリ 3 にアクセスして新たに発行された C R L 7 を取得する処理を省くことができる。

【0130】

また、本実施例では、上記 C R L 発行通知 8 の送信や、上記 C R L 発行通知依頼メッセージ 10 の受信は、上記認証局 1 が行うようにしているが、本発明はそれに限定されるものではない。例えば、上記 C R L 発行通知 8 の送信や、上記 C R L 発行通知依頼メッセージ 10 の受信を上記 C R L リポジトリ 3 が行うようにしてもよい。

【0131】

あるいは、C R L リポジトリ 3 に、上記 C R L 7 の発行を監視し、新たな C R L 7 が発行されたことを確認した場合に上記 C R L 発行通知 8 を送信する機能を実現する C R L 発行確認ソフトウェアを導入し、さらに当該 C R

L 発行確認ソフトウェアは上記 C R L 発行通知依頼受信機能を実現し、上記 C R L 発行通知送信機能は、受信した上記 C R L 発行通知依頼メッセージの送信元に、上記 C R L 発行通知を送信するようにしてもよい。

【0132】

上記 C R L 発行確認ソフトウェアを利用することで、上記 C R L 発行通知送信機能を持たない上記認証局 1 や上記 C R L リポジトリ 3 をも利用することが可能になる。さらに、上記 C R L 発行通知依頼受信機能が上記 C R L 発行通知の送信先を管理すれば、上記 C R L リポジトリの運営者と上記証明書検証サーバの運営者とが異なっても上記証明書検証サーバの数を柔軟に変更することができる。

【0133】

本実施例によれば、上記 C R L 発行通知は上記認証局が上記 C R L を発行した時に当該認証局から上記証明書検証サーバに対して行われるだけであるので、一定時間毎に上記 C R L が発行されているかどうかを確認する必要がなく、ネットワーク 0 にかかる負荷が小さくて済む。

20 【0134】

また、上記 C R L 発行通知 8 は上記認証局 1 によって行われるため、上記 C R L リポジトリ 3 と、上記証明書検証サーバ 4 の運営者が異なる場合でも、高い精度の証明書有効性検証を行うことができる。

【0135】

さらに、上記証明書検証サーバ 4 は、上記 C R L 発行通知依頼メッセージ 10 を送信することにより上記 C R L 発行通知 8 の送信を依頼することができるため、上記 C R L リポジトリ 3 の運営者と上記証明書検証サーバ 4 の運営者とが異なっても上記証明書検証サーバ 4 の数を柔軟に変更することができる。

【0136】

さらに、上記証明書検証サーバが新たな C R L が発行されたことを発見した場合、当該証明書検証サーバが他の証明書検証サーバに新たな上記 C R L が発行されたことを通知する。

【0137】

送信する上記証明書検証サーバを変更したい場合には、当該証明書検証サーバの設定を変更すればよい。また、上記 C R L リポジトリの運営者と上記証明書検証サーバの運営者とが異なっても上記証明書検証サーバの数を柔軟に変更することができる。

【0138】

さらに、上記証明書検証サーバが、検証パスを新たに構築した場合、当該検証パスを他の証明書検証サーバにも転送し、検証パスを共有するため、特定の上記 C R L リポジトリや上記証明書リポジトリへのアクセスの集中や、ネットワーク負荷を抑えることができる。

【0139】

50 また、上記証明書を別途入手する方法を利用した場合に

も、上記クライアントは、上記証明書リポジトリにアクセスして上記証明書を取得するのではなく、上記証明書検証サーバに、上記証明書を取得し、かつ、当該証明書の有効性を検証するように依頼するため、クライアントに、上記証明書リポジトリにアクセスして上記証明書を取得する機能を実装する必要がない。

【0140】

【発明の効果】

したがって、本発明によれば、上記証明書の有効性検証を高い精度と少ない負荷で確実にこなうことができる。

【図面の簡単な説明】

【図1】本発明の一実施形態が適用された、電子署名付き電子文書交換システムのシステム構成を示す図である。

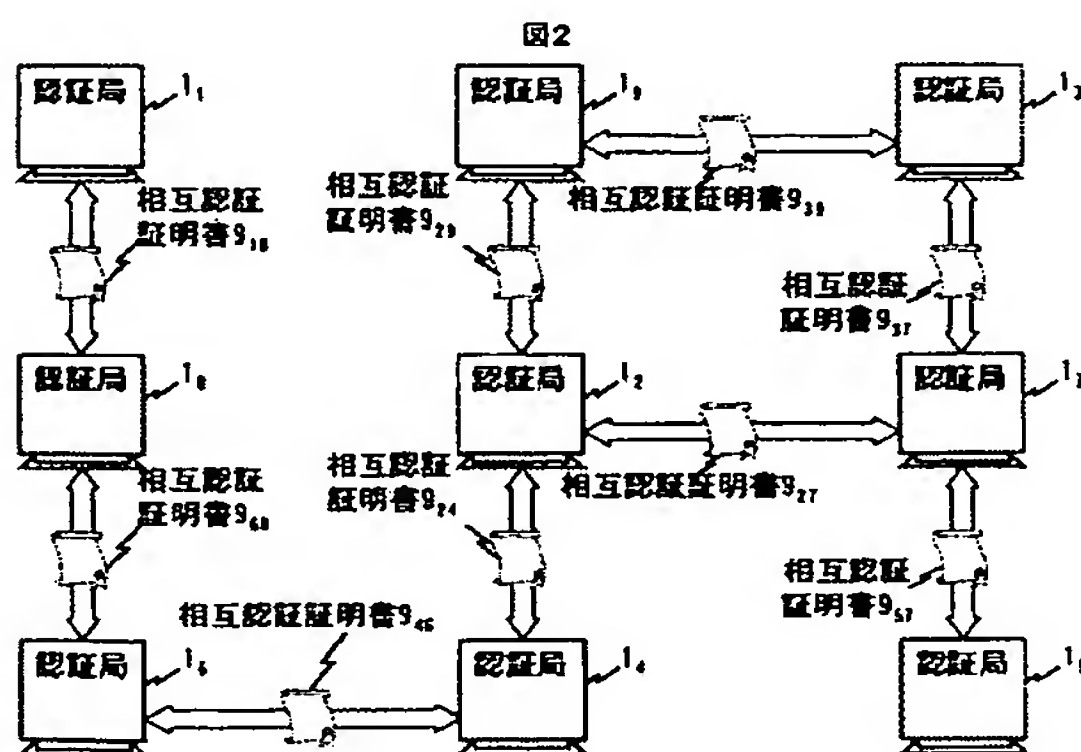
【図2】図1の電子署名付き電子文書交換システムにおいて、認証局1間の相互認証の関係を示す図である。

【図3】図1の電子署名付き電子文書交換システムにおいて、CRL7が発行された場合の動作を示す図である。

【図4】図1の電子署名付き電子文書交換システムにおいて、証明書509が電子文書とともに送付される場合に、クライアント端末5が電子文書6を送受する際の動作を示す図である。

【図5】図1の電子署名付き電子文書交換システムにおいて、証明書509が電子文書とともに送付されない場合に、クライアント端末5が電子文書6を送受する際

【図2】



の動作を示す図である。

【図6】CRL発行通知送信先リスト104と、CRL発行通知転送先リスト408の一例を示す図である。

【図7】図1の電子署名付き電子文書交換システムにおいて、証明書検証サーバ4が認証局1に対してCRL発行通知8の送信を依頼する場合の動作を示す図である。

【図8】CRL発行通知依頼メッセージ10の一例を示す図である。

【図9】図1に示す認証局1、証明書リポジトリ2、CRLリポジトリ3、証明書検証サーバ4、クライアント端末5の各々のハードウェア構成例を示す図である。

【符号の説明】

0・・・ネットワーク、1、1₁～1₉・・・認証局、2・・・証明書リポジトリ、3・・・CRLリポジトリ、4、4₁～4_n・・・証明書検証サーバ、5、5₁～5_m・・・クライアント端末、6・・・電子文書、7・・・CRL、8・・・CRL発行通知、9・・・相互認証証明書、10・・・CRL発行通知依頼メッセージ、91・・・CPU、92・・・メモリ、93・・・外部記憶装置、94・・・読取装置、95・・・通信装置、96・・・入力装置、97・・・出力装置、98・・・インターフェース、99・・・記憶媒体、104・・・CRL発行通知送信先リスト、408・・・CRL発行通知転送先リスト、409・・・検証パス送信先リスト、508、508₁～508_m・・・秘密鍵、509、509₁～509_m・・・証明書。

【図3】

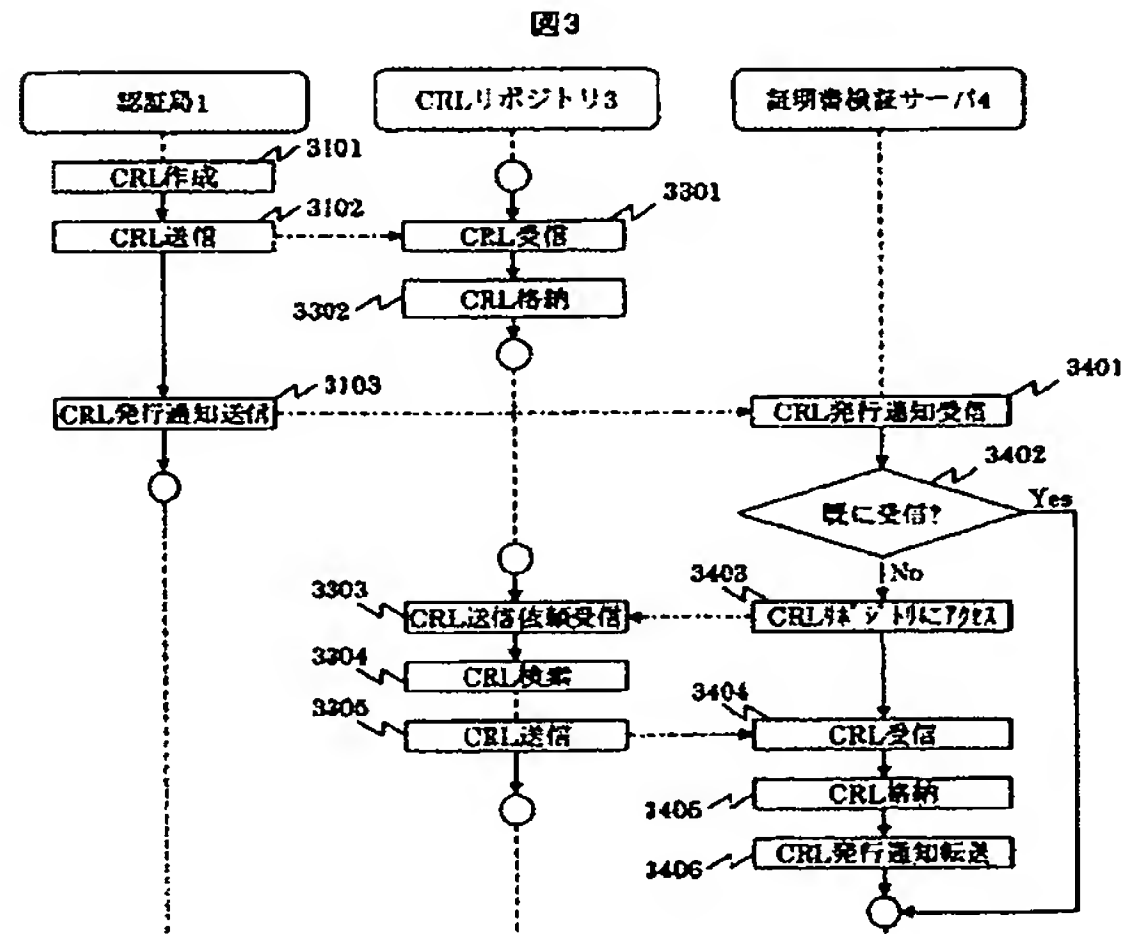
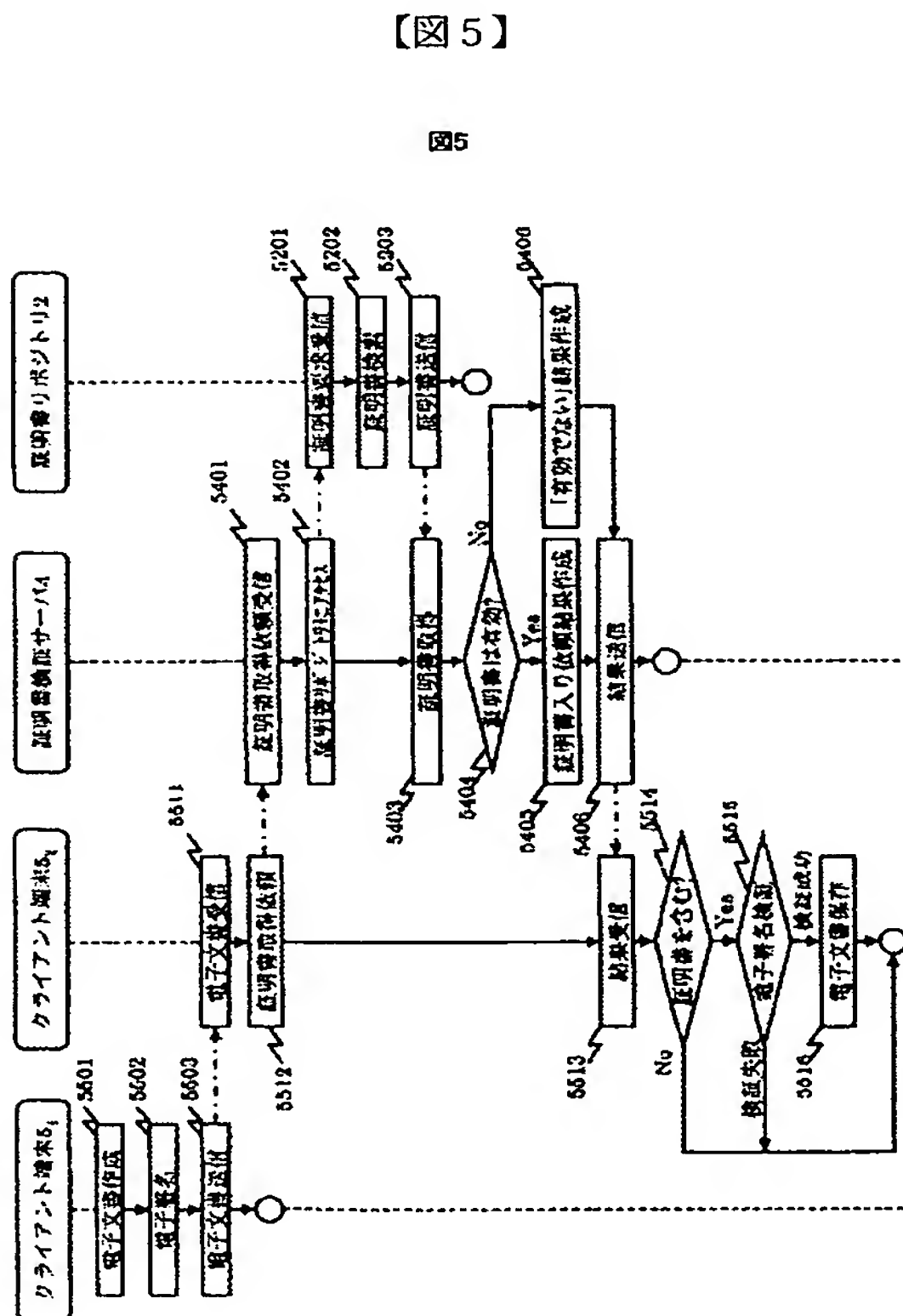
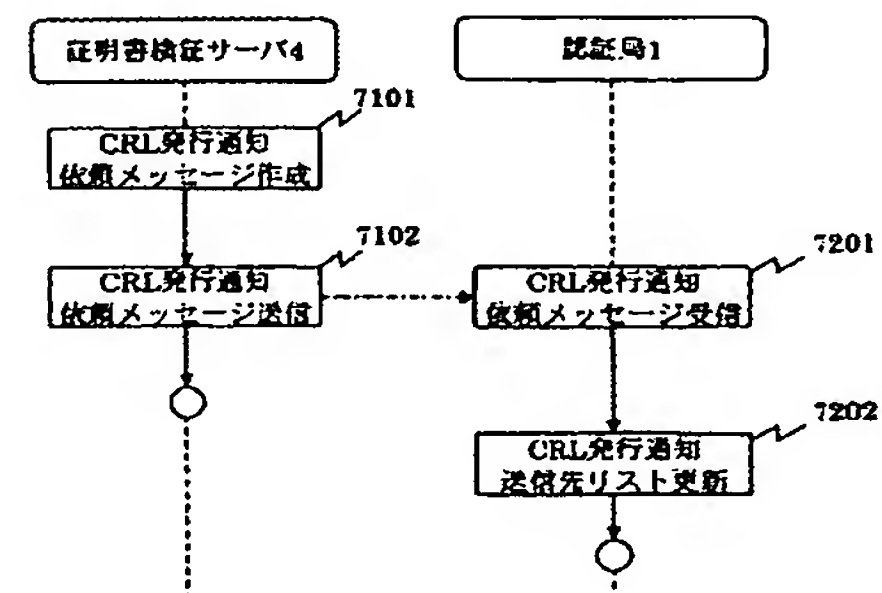
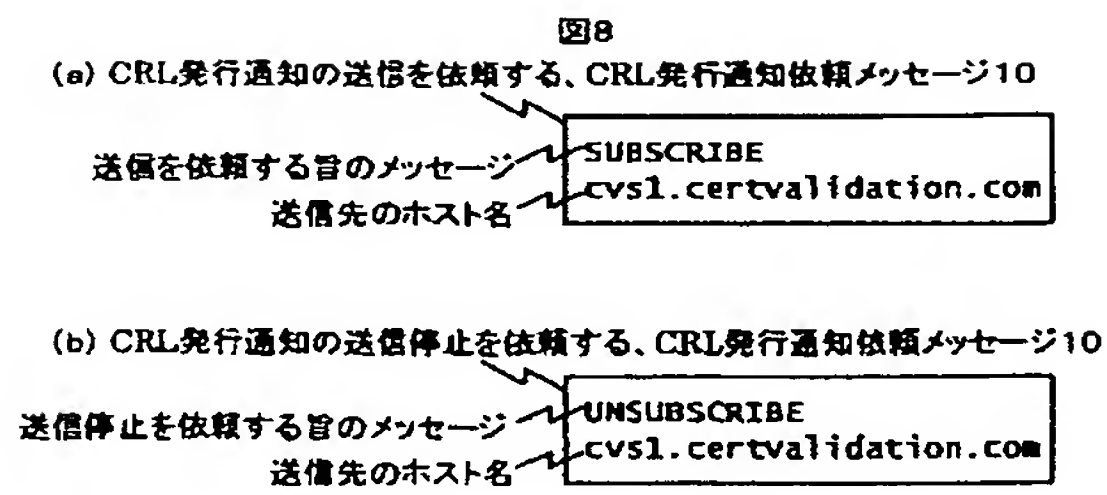


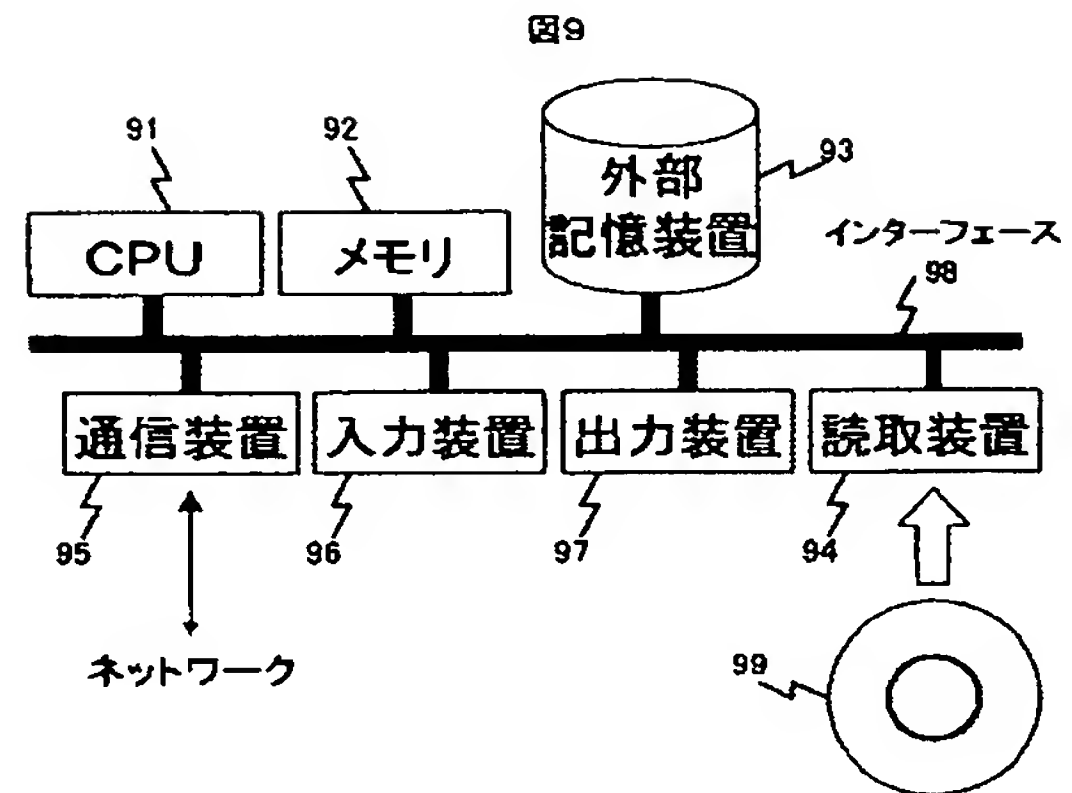
图7



【図8】



【図9】



フロントページの続き

(72)発明者 熊谷 洋子

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 羽根 慎吾

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 長野 裕美

東京都江東区新砂一丁目6番27号 株式会社日立製作所公共システム事業部内

Fターム(参考) 5J104 AA16 EA05 MA01